Avvik og avvikshåndtering Kontrollkommisjonene

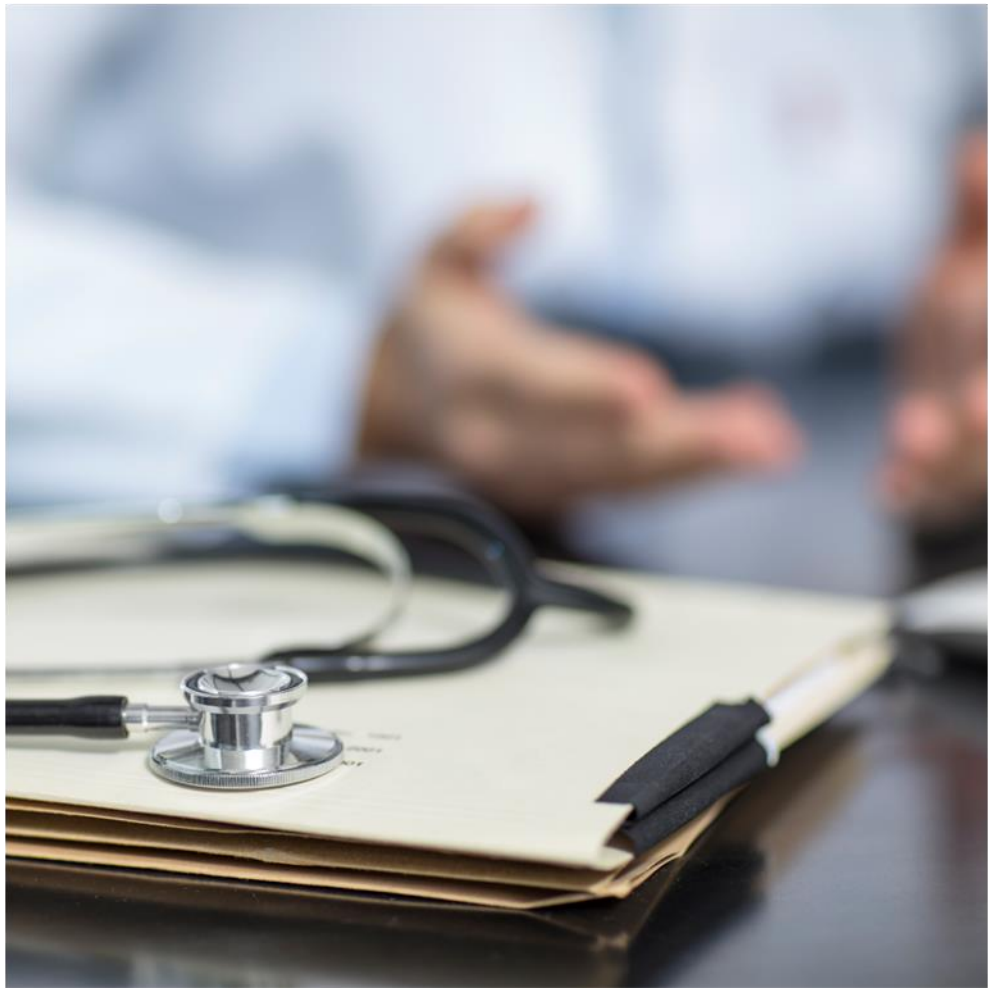
Britt Eva Haaland, Personvernombud

Personvern og avvikshåndtering

Del 1- Generelt om personvern

Del 2- Hva er et avvik/sikkerhetsbrudd?

Del 3- Hvordan skal avvik/sikkerhetsbrudd håndteres?



C2 - Restricted use

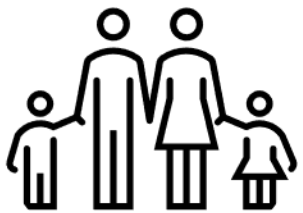
Del 1 – Generelt om personvern

Hva er personvern?

Personvern handler om retten til å bestemme over egne personopplysninger og retten til et privatliv

Grl § 102

"Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet"



EMK art 8

"Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse"

Retten til å bestemme over egne personopplysninger er styrket etter GDPR.

C2 - Restricted use

Hva er personvern?

Personvern handler om enkeltpersoners rett til å ha innflytelse på bruk og spredning av personopplysninger om seg selv

Det er den personen som opplysningene handler om som eier opplysningene

C2 - Restricted use

Hva er en personopplysning?

En personopplysning er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson

- Navn,
- Fødselsnummer
- Adresse

- Bilder
- Fingeravtrykk
- Irismønster
- Hodeform

Adferdsmønster

Helseopplysninger

Og mye mer.....

C2 - Restricted use

Hva vil det si å behandle personopplysninger?

All bruk av personopplysninger er behandling

…også det å "bare ha dem" og uavhengig av om mennesker er involvert i behandlingen eller om det skjer automatisk

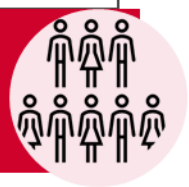
C2 - Restricted use

Del 2 – Hva er et avvik/sikkerhetsbrudd?

Et sikkerhetsbrudd består av tre elementer

Sikkerhetsbruddet må gjelde personopplysninger

Personopplysninger



Det må være et brudd på konfidensialitet, integritet eller tilgjengelighet

Sikkerhetsbrudd

Sikkerhetsbruddet må føre til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger

Årsakssammenheng

Skjer det et brudd på konfidensialitet, integritet eller tilgjengelighet foreligger det et avvik.

Et avvik er et sikkerhetsbrudd.

Et sikkerhetsbrudd er altså når personopplysninger er kommet på avveie, når opplysninger kan ha blitt forandret eller når personopplysninger ikke lenger er tilgjengelige for de som behøver dem.

C2 - Restricted use

Må gjelde personopplysninger

Det må være personopplysninger
som er berørt, for at noe skal ansees
som et sikkerhetsbrudd i
personvernssammenheng.

Andre opplysninger vil ikke utløse
meldeplikt til Datatilsynet

C2 - Restricted use

Det er tre former for sikkerhetsbrudd

Brudd på konfidensialitet

At informasjon har konfidensialitet betyr at informasjonen er sikret og at informasjonssystemene bare er tilgjengelige for de som har et tjenstlig behov.

Personopplysningene skal være sikret mot at uvedkommende får adgang til opplysningene

Brudd på integritet

At informasjon har integritet betyr at det er sikret at informasjonen er korrekt, gyldig og fullstendig, og at den ikke kan endres utilsiktet eller av uvedkommende.

Personopplysningene skal være sikret mot utilsiktete eller uautorisert ødeleggelse, endring eller sletting

Brudd på tilgjengelighet

Dette betyr at informasjon og informasjonssystemer er sikret og at informasjon er tilgjengelige ved behov innenfor de krav som er satt.

Personopplysningene skal være tilgjengelige for det tiltenkte formålet

C2 - Restricted use

Det må være en årsakssammenheng

GDPR art 4 nr.12

«...brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet».

Hva innebærer det?

Det må være en årsakssammenheng mellom sikkerhetsbruddet og konsekvensen

Eksempler på sikkerhetsbrudd

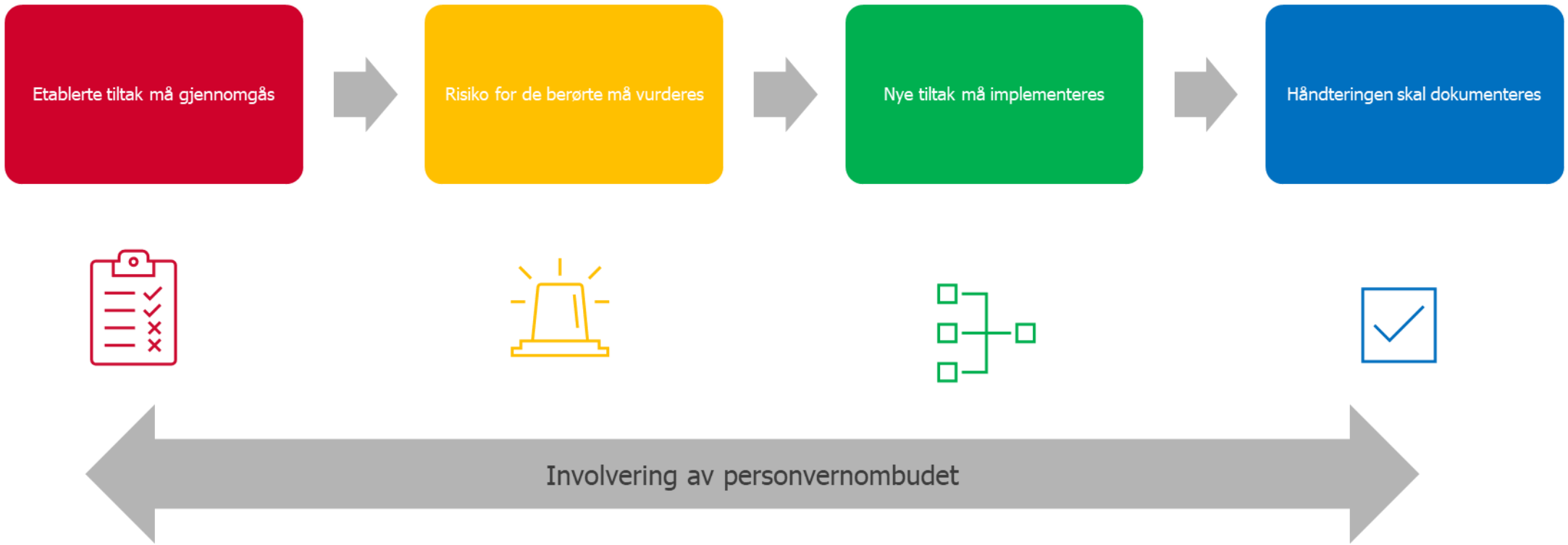
- Sending av post/e-post til feil mottaker
- Mangler eller feil i tilgangsstyringen
- Utilsiktet publisering av personopplysninger
- Hacking/datainnbrudd
- Papirdokumenter som er gått tapt, blitt stjålet eller etterlatt
- E-post/brev som har blitt åpnet av feil person
- Muntlig utlevering av personopplysninger som ikke skulle ha skjedd
- Tapt eller stjålet enhet (smarttelefon, datamaskin, back-up harddisk)
- Personopplysninger lagret på gamle enheter som feilaktig kastes
- Datavirus/malware (for eksempel programmer som krypterer filene på datamaskinen, og man må betale for å få tilbake tilgangen)

C2 - Restricted use

Del 3 – Hvordan skal avvik/sikkerhetsbrudd håndteres?

4 steg ved håndtering av avvik

For nærmere beskrivelse av hvert steg, se følgende slides



C2 - Restricted use

Etablerte tiltak må gjennomgås

Hvis det oppdages brudd på personopplysnings-sikkerheten
må Kontrollkommisjonen vurdere om tekniske og organisatoriske tiltak er effektive og fungerer som de skal

Dersom tiltakene er mangelfulle må det iverksettes nye tiltak som
sikrer at personvern-forordningen blir oppfylt, og som sikrer de berørtes rettigheter og friheter

Nye tiltak må dokumenteres og følges opp med informasjon/ opplæring

Eks. tekniske tiltak:
Kryptering av dokumenter, passordbeskyttelse, sladding av dokumenter, fysisk sikring

Eks. org. tiltak:
Relevant opplæring, driftsmessige prosedyrer, tilgangsstyring, prosedyrer for eksterne aktører

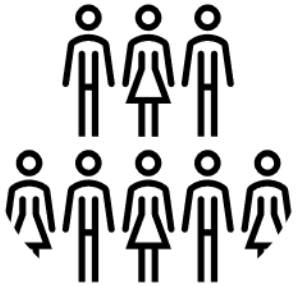
C2 - Restricted use

Risiko for de berørte må vurderes

1. Er personopplysninger omfattet av bruddet?
2. Innebærer sikkerhetsbruddet en risiko for enkeltpersoners rettigheter og friheter?
3. Skal Datatilsynet og de berørte varsles, og skal Helsedirektoratet orienteres?

C2 - Restricted use

Er personopplysninger omfattet av bruddet?



Sikkerhetsbruddet omfatter personopplysninger

Et brudd på sikkerheten er ikke alltid et brudd på personopplysningssikkerheten.

Sikkerhetsbruddet må omfatte *personopplysninger* for at sikkerhetsbruddet skal utløse varslingsplikt.

Sikkerhetsbruddet innebærer personvernrisiko

Sikkerhetsbruddet må medføre **moderat** eller **høy risiko** for de registrertes rettigheter eller friheter for å utløse varslingsplikt til Datatilsynet. Dette betyr at det gjøres unntak fra varslingsplikten dersom virksomheten vurderer at sikkerhetsbruddet har **lav personvernrisiko**.

C2 - Restricted use

Innebærer sikkerhetsbruddet en risiko for enkeltpersoners rettigheter og friheter?

I risikovurderingen skal du vurdere hvilke konsekvenser sikkerhetsbruddet kan få for de registrerte, og sannsynligheten for at disse konsekvensene inntreffer.

Eksempler på konsekvenser kan være tap av kontroll på egne helseopplysninger, skade på omdømme og tap av fortrolighet for taushetsbelagte personopplysninger.

C2 - Restricted use

Innebærer sikkerhetsbruddet en risiko for enkeltpersoners rettigheter og friheter?

Når personvernrisikoen vurderes er det viktig å ta i betraktning under hvilke omstendigheter sikkerhetsbruddet oppstod

Hva slags type sikkerhetsbrudd har skjedd? F.eks. tyveri, hacking, snoking, tap av papirdokumenter, brudd på interne rutiner etc.	Har det skjedd et brudd på konfidensialitet, integritet eller tilgjengelighet?	Medfører sikkerhetsbruddet brudd på andre bestemmelser i GDPR?	Hvilke typer personopplysninger er berørt av bruddet?	Hvor lett er det å identifisere pasientene ut fra opplysningene som er kommet på avveie?	Berører sikkerhetsbruddet sårbare grupper – som barn, psykisk syke, rusavhengige eller andre utsatte grupper som bruddet kan ha spesielt store konsekvenser for?	Hvor mange registrerte er berørt av sikkerhetsbruddet – en, få eller mange?

C2 - Restricted use

Skal Datatilsynet og/eller de registrerte varsles?

Resultatet av risikovurderingen er avgjørende for *om* det skal varsles og *hvem* som eventuelt skal varsles om sikkerhetsbruddet

Ingen eller lav risiko
= Ingen varsling er påkrevd

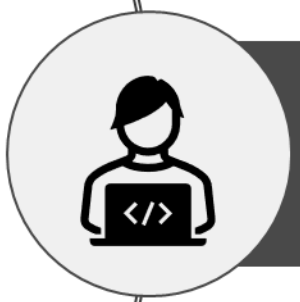
Moderat risiko
= Datatilsynet skal varsles

Høy risiko
= Datatilsynet og de registrerte skal varsles

C2 - Restricted use

Hva skal melding til Datatilsynet og de berørte inneholde?

Hva som har skjedd og hva slags type sikkerhetsbrudd det er snakk om



Hvilke konsekvenser sikkerhetsbruddet kan ha for de registrerte (f.eks. skade på de registrertes omdømme, tap av kontroll på egne helseopplysninger etc.)

Hvilke tiltak Kontrollkommisjonen har iverksatt for å håndtere sikkerhetsbruddet og redusere eventuelle skadevirkninger det måtte ha for den registrerte

I tillegg skal det opplyses om navn og kontaktopplysninger til personvernombudet eller annen person i Kontrollkommisjonen som kan gi mer informasjon om sikkerhetsbruddet.

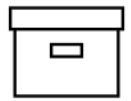
C2 - Restricted use

Eksempler på sikkerhetsbrudd som skal meldes til Datatilsynet

Brev eller e-post som inneholder personopplysninger er sendt til feil mottaker.

Angrep mot datasystemer (hacking) hvor personopplysninger har blitt hentet ut, er endret på eller er utilgjengelige, eller at det er sannsynlig at dette har skjedd.

Kastede dokumenter som skulle vært makulert.



Forsendelser til riktig mottaker, som ved en feil inneholder beskyttelsesverdige personopplysninger om andre personer.

Det blir oppdaget sikkerhetshull, og Kontrollkommisjonen kan ikke utelukke at uvedkommende har utnyttet seg av det.

Mistet, frastjålet eller gjenglemt:

- Papirdokument
- Datamaskin, nettbrett eller telefon der innholdet ikke er kryptert
- Minnepinne eller lignende der innholdet ikke er kryptert

Postforsendelser hvor emballasjen er åpnet.

Uautorisert eller utilsiktet publisering av personopplysninger som ikke skulle ha vært publisert, eller at personopplysningene ikke har blitt anonymisert.

Datatilsynet kan varsles via postkasse@datatilsynet.no eller via alminnelig brevpost.

For ytterligere eksempler se EDPBs retningslinjer «Guidelines 01/2021 on Examples regarding Personal Data Breach Notification»

C2 - Restricted use

Hvem skal ha beskjed om avviket?

Datatilsynet

Datatilsynet skal varsles uten ugrunnet opphold derom sikkerhetsbruddet medfører moderat eller høy risiko, og senest innen 72 klokketimer.
Dersom bruddet ikke meldes innen 72 timer, skal årsakene til forsinkelsen oppgis til Datatilsynet.

De berørte

De berørte skal varsles uten ugrunnet oppholdet dersom sikkerhetsbruddet medfører høy risiko for de registrertes rettigheter og friheter.

Datatilsynet kan varsles via postkasse@datatilsynet.no eller via alminnelig brevpost.

Vær oppmerksom på at pasientopplysninger ikke kan sendes på e-post, men en generell, anonymisert melding kan sendes pr e-post

Personvernombudet skal involveres

Når avvik oppstår bør personvernombudet involveres så tidlig som mulig.
E-posten til personvernombudet er
personvernombud.kontrollkommisjonen@helsedir.no

Når skal Helsedirektoratet orienteres?
Hvis det er omfattende avvik, risiko for medieomtale eller andre forhold som tilsier det, skal Kontrollkommisjonens leder også varsle Helsedirektoratet v/avdeling helserett og rettssaker pr telefon.

Kopi av avviksmeldinger til Datatilsynet sendes alltid kontrollkommisjonen@helsedir.no

C2 - Restricted use

Forut for lukking av avviket må nye tiltak identifiseres og implementeres

Når etablerte tiltak er gjennomgått og risikoen er vurdert, må risikoreduserende tiltak identifiseres og implementeres.

Nye tiltak må dokumenteres og følges opp med informasjon/opplæring.

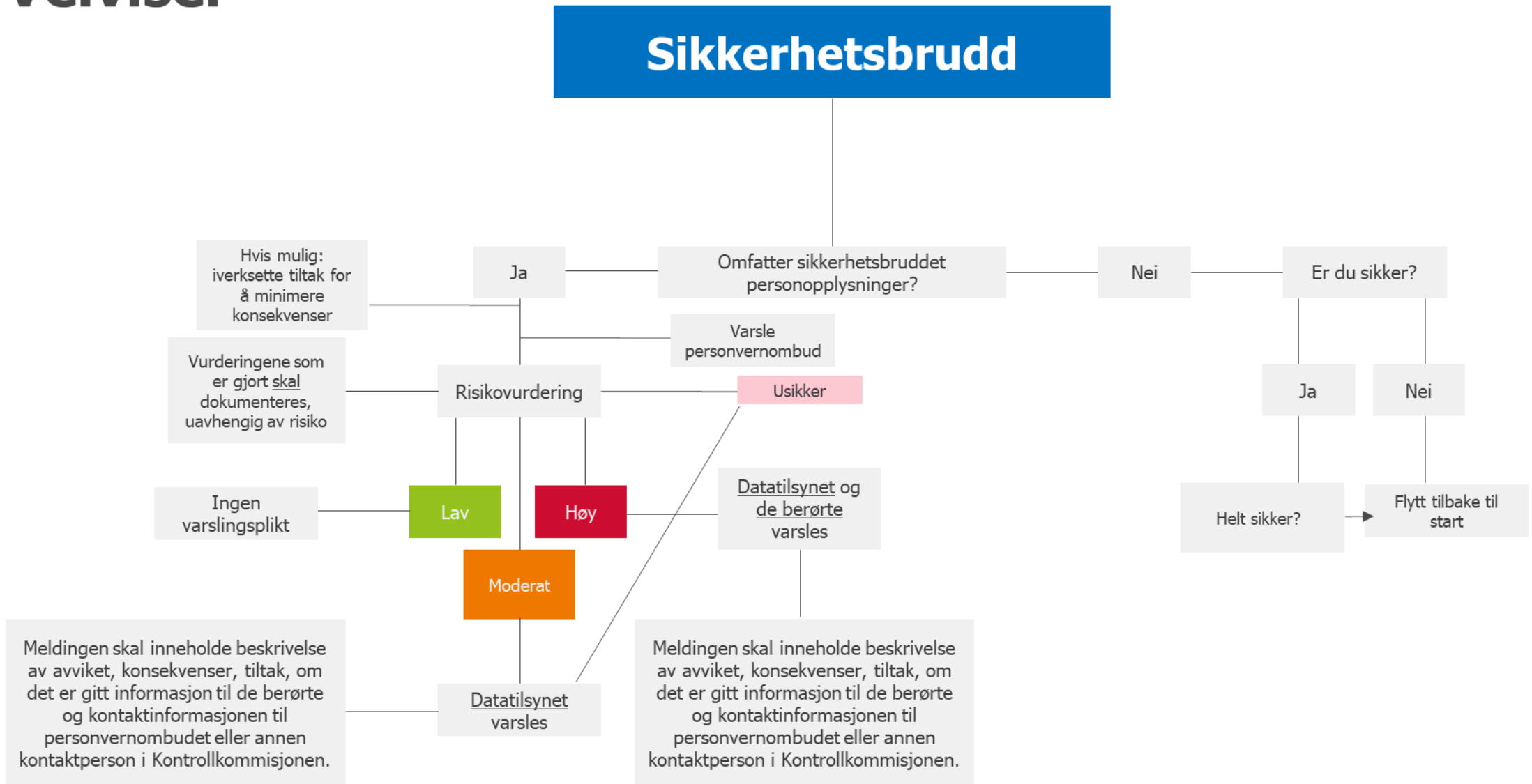
C2 - Restricted use

Vurderingene som er gjort skal alltid dokumenteres

Selv om du kommer til at det ikke er nødvendig å varsle Datatilsynet eller de registrerte – det vil si at det foreligger lav personvernrisiko – er det viktig å dokumentere de vurderinger som er gjort.

C2 - Restricted use

Veiviser



C2 - Restricted use

Oppsummering

Kommisjonens medlemmer har ansvar for å identifisere og melde avvik til nærmeste leder/personvernombud.

Datatilsynet skal varsles uten ugrunnet opphold derom sikkerhetsbruddet medfører moderat eller høy risiko, og senest innen 72 klokketimer. Dersom bruddet ikke meldes innen 72 timer, skal årsakene til forsinkelsen oppgis til Datatilsynet.

De registrerte skal varsles, dersom sikkerhetsbruddet medfører høy risiko.

Når det oppdages et avvik skal medlemmene - om mulig - igangsette tiltak for å minimere konsekvenser.

Meldingen til Datatilsynet skal inneholde beskrivelse av avviket, konsekvenser, tiltak, om det er gitt informasjon til de berørte og kontaktinformasjonen til personvernombudet eller annen kontaktperson i virksomheten.

Uavhengig av hvorvidt sikkerhetsbruddet er varslingspliktig eller ikke, må bruddet og vurderingen som er gjort dokumenteres.

Personvernombudet skal varsles uten ugrunnet opphold (dette gjelder i og utenfor arbeidstid).

Om ikke all info foreligger på meldingstidspunktet kan informasjon ettersendes. Dette må i så fall opplyses om i første melding.

Datatilsynet kan varsles via postkasse@datatilsynet.no eller via alminnelig brevpost.

Kopi av melding til Datatilsynet sendes til kontrollkommisjonen@helsedir.no

Ved omfattende avvik, risiko for medieoppmerksomhet e.l skal leder også varsle helsedirektoratet v/avdeling helsrett og rettssaker pr telefon

C2 - Restricted use

Etter dette kurset skal du vite

Hva et avvik er

Hvordan du gjenkjenner et avvik

Hvem du skal snakke med hvis du oppdager et avvik

Hvilke plikter du har når et avvik oppstår

C2 - Restricted use